TTP: Transient Tunneling Procedure for Dynamic Home Addressing on Mobile Hosts

Sandra Thuel, Tom La Porta, Ram Ramjee, Luca Salgarelli and Kannan Varadhan
Lucent Technologies, Bell Laboratories

Abstract

Dynamic home addressing has lately become a popular and viable approach to configuring mobile IP hosts. This paper introduces a method for mobile hosts to dynamically acquire a home address through DHCP when powering up in a foreign domain, referred to as the Transient Tunneling Procedure (TTP). TTP is proposed as a solution to a recently observed problem, namely, that mobile hosts cannot rely on standard DHCP broadcasting procedures to properly discover an addressing server in their home network. TTP requires minor changes to protocol standards and deployed servers and it leverages the growing base of DHCP technology, with its embedded support for important configuration options besides IP addressing. We present the TTP message flows as well as standard procedures needed to acquire and maintain network connectivity on hosts as they roam. We show implementation results, discuss alternative solutions and other related issues impacting dynamic addressing on mobile hosts such as configuration latency and wireless bandwidth usage.

1. Introduction

An integral part of supporting seamless mobility for a host connected to the Internet is the ability to configure its IP address to match that of the subnet onto which it is attached at any point in time. Having the correct IP address is needed to ensure that IP packets get routed to the host. The Mobile-IP protocol (M-IP) [5] provides a solution for transparent mobility which prevents application disruption as IP address changes take place when a host moves. In M-IP, a mobile host (MH) has a fixed IP *home address* and acquires an additional IP *care-of address* (COA) that is updated as the host changes its point of attachment. While M-IP relies on the ability to configure these addresses, it does not dictate how they are to be obtained.

Traditionally, it has been assumed that MH's have a *fixed* home address that is statically configured. More recently, the trend has been to shift to a *dynamic* home addressing model, where a dynamic configuration protocol enables MH's to acquire and install a home address on power-up. Dynamic home addressing enables an efficient management of IP addresses, which is critical in supporting wide-area wireless data users with millions of devices using a limited Ipv4 address space. It also provides ease of configurability by replacing the burdensome task of manually configuring hosts with a more effective mechanism of allocating IP addresses. There are similar arguments to support the dynamic allocation of COAs. This approach is valuable to MH's that are equipped with a *co-located* M-IP foreign agent (FA), which requires the MH to acquire a globally unique IP COA on handoffs. While the adoption of FA co-location on the MH is controversial and virtually independent of the dynamic home addressing problem, it illustrates another area where dynamic addressing plays a critical role.

DHCP is the current dynamic addressing and configuration protocol in widespread use on the Internet [6]. It not only enables hosts to acquire IP addresses but also other configuration parameters known as *DHCP options* associated with the access network (e.g., netmask for subnet, domain name servers such as DNS or WINS, directory servers such as NDS, email servers such as SMTP and POP3, etc. [9]). As emerging and future client applications increasingly rely on network services, the ability to dynamically configure these services through DHCP options becomes important. DHCP has already become a popular tool for ISP's to manage the addressing needs of their dial-up users. It is likewise a natural candidate to support dynamic addressing on mobile hosts. However, DHCP was designed for fixed IP hosts and its use on mobile hosts presents a number of challenges.

Many of DHCP's limitations in supporting mobile hosts have been well documented in the literature [1,2,3,12]. Main issues concern DHCP's configuration latency, its effective use of wireless bandwidth, and security (a concern not exclusive to mobile hosts). These issues are relatively well-known and there has been on-going work to address them. A problem, however, that has not been addressed is that the standard DHCP procedures for dynamic home addressing on mobile hosts do not work under some circumstances. Specifically, mobile hosts that power up in a foreign network cannot rely on standard DHCP broadcast messages on the access subnet to reach a DHCP server in their home networks for acquiring an address. By the same token, a mobile host in a foreign network cannot successfully broadcast DHCP messages to renew its home address lease. This problem has only recently emerged because dynamic home addressing is a novel enhancement proposed for Mobile IP hosts.

The thrust of this paper is to describe this *DHCP broadcasting problem* and to provide an in-depth solution referred to as the *Transient Tuneling Procedure* (TTP). TTP comprises a two-stage addressing procedure for mobile hosts that power up in a foreign network. It introduces the notion of an addressing element referred to as a *bootstraping agent* co-located with a M-IP Home Agent for the temporary creation of a tunnel over which standard DHCP transactions take place. We describe the set of transactions that are needed to acquire and maintain connectivity on mobile hosts as they roam. Our model assumes that a mobile host uses DHCP to dynamically acquire both a home address and a co-located COA. However, it is also applicable to the case where a COA is obtained by other means (e.g., via a non-colocated foreign agent). We discuss alternative solutions and other related issues impacting dynamic addressing such as wireless bandwidth usage and the use of external Foreign Agents.

A key benefit of TTP is that it requires minor changes to protocol standards and deployed servers, amounting to a few enhancements to the M-IP protocol and Home Agents. In addition, TTP leverages the growing base of DHCP technology and its embedded support for important and often necessary DHCP configuration options beyond IP addressing (e.g., subnet mask, DNS servers, etc.). While being DHCP-based, TTP is potentially useful to any dynamic home addressing protocol that, like DHCP, relies on broadcasting for server discovery. Although TTP is not needed for hosts powering up in their home network, power-ups in a foreign network are expected to be the more frequent case (e.g., use of M-IP for corporate access).

The paper is organized as follows. In Section 2, we describe prior work concerning the support for dynamic addressing on mobile hosts. In Section 3, we provide an overview of the Mobile-IP and DHCP protocols. Section 4 describes the DHCP broadcasting problem and Section 5 introduces our dynamic addressing solution involving both Mobile-IP and DHCP. In Section 6, we describe our implementation work. Sections 7 and 8, respectively, present alternative solutions and other related issues concerning DHCP and mobility. We conclude with a summary and suggestions for future work in Section 9.

2. Related Work

There have been several efforts to address DHCP's limitations regarding its support for host mobility. Perkins and Luo [1] give an early account of the problems concerning the use of DHCP on portable and mobile hosts. They highlight problems affecting DHCP irrespective of mobility, such as administration issues, its lack of security and a dynamic DNS mechanism to enable the location of dynamically addressed hosts. DHCP security and dynamic DNS have been the subjects of considerable investigation and are still under the scrutiny of the IETF [15,16,13]. Specific to mobility, they suggest the co-location of DHCP servers with M-IP home agents and DHCP relays with M-IP foreign agents, for performance and administration improvements. They also refer to the use of dynamic home agent allocation, an option that has since been added to the DHCP standard [17]. However, they do not consider dynamic home addressing for mobile users, which is the focus of this paper. Vatn and Maguire [2] examine the use of DHCP to dynamically acquire a co-located COA. They measure the corresponding increase in handoff latency and suggest means to eliminate DHCP's address conflict checking mechanism as a means to reduce configuration latency.

A recent IETF draft proposes the Dynamic Registration and Configuration Protocol (DRCP), a DHCP-like protocol aimed at addressing a number of issues concerning DHCP's inadequacy for mobile hosts [12]. DRCP does not examine dynamic home addressing but instead targets issues such as performance, network configurability, and Quality of Service (QoS). In doing so, it proposes major changes to the DHCP standard and it introduces several features that are potential pitfalls. DRCP replaces the stateless DHCP relays with stateful DRCP proxies or virtual servers containing caches to aid in reducing lease acquisition and renewal latencies when actual servers are involved. The population of cache entries introduces control traffic between servers and proxies and the management of proxy failures is an open issue. DRCP also includes support for QoS negotiation and mobility detection, increasing control traffic over the wireless link (e.g., router advertisements). We contend that most of the mobility issues DRCP intends to address can and should be addressed without significant changes to the DHCP standard. Moreover, the cost of embedding QoS and mobility detection into DHCP is not justified, especially on mobile host configurations which already rely on the use of specialized protocols to manage this (e.g., M-IP).

Contrasting with work on DHCP and mobility, Calhoun and Perkins [4] are among the first to examine M-IP and dynamic addressing. They introduce an architecture for dynamic home addressing that relies on M-IP messages and an abstract element in the home network referred to as the Home Domain Allocation Function (HDAF). They extend M-IP registration messages to enable the use of a Network Access Identifier or NAI (e.g., an email address) to identify a mobile user rather than using a mobile host IP address. It is suggested that a M-IP registration message with a NAI extension sent by a mobile host can be used (e.g., by a M-IP FA) to locate the HDAF. Details on how to locate the HDAF and on how the HDAF actually allocates home addresses are left as open issues. This work assumes the use of an external FA, where a simple dynamic home addressing scheme to only acquire an IP address is viable though it will not work in the more general case where a non-colocated FA is used.

Though not targeted at mobile hosts, Patel, et.al [14] describe a method for fixed IP hosts to connect to a remote corporate network via an IP Security tunnel (IPSec) over which they conduct DHCP transactions to configure the remote host. Their model relies on the existence of a Virtual Private Network (VPN) server in the home network that the host must know about, which has been modified to also serve as a DHCP relay on behalf of the host. Mobile-IP is not used.

The DHCP broadcasting problem this paper focuses on surfaced as a key hurdle to overcome in realizing and implementing an architecture in the spirit of the HDAF, though specifically using

DHCP for address allocation and M-IP for mobility. In spite of the issues concerning DHCP's support for mobility, there is much on-going research to strengthen its weaknesses. It has already received widespread commercial support and it is flexible enough (with DHCP options) to support current and future dynamic host configuration needs beyond simple addressing. Consequently, we advocate dynamic home addressing solutions based on DHCP.

3. Background

3.1. Mobile-IP Overview

In a Mobile IP network there are two mobility agents: a *home agent* and a *foreign agent* [5]. A Home Agent (HA) provides mobility support for mobile hosts that belong to this home network while a Foreign Agent (FA) serves hosts that are visiting from a remote home network. A mobile host attaches to the network through an access router. Each mobile host must have an IP address known as its *home address*. When a mobile host is attached to a foreign network it requires a second IP address known as the *care-of address (COA)*. The manner in which the COA is assigned depends on whether the FA resides on the MH, known as the *co-located COA* option or on an a device in the local access network. When an FA is used, the COA is the IP address of one of its interfaces. In the case of co-location, the MH acquires a COA through static means or preferably through a dynamic addressing protocol like DHCP.

Packets sent to the mobile host by a corresponding host are always addressed to the home address of the mobile node. While the mobile host is attached to its home network, packets reach it following conventional IP routing which is based on the subnet portion of the mobile's home address. When the mobile host moves into a foreign network, it must acquire a COA and register it with its home agent. Once registered, packets destined to the home address of the mobile host are routed through the Internet as normal IP packets until they reach the home network of the mobile device. In the home network, the home agent of the mobile device intercepts these packets. The home agent encapsulates these packets inside packets that are addressed to the care-of address of the mobile device. These packets are then routed on the Internet as normal IP packets until they reach the foreign agent corresponding to the mobile device. In this way packets are *tunneled* through the network. The foreign agent decapsulates the original IP packets and forwards them to the mobile device. Packets sent from the mobile device may be treated as normal IP packets or they may be *reverse-tunneled*, that is, encapsulated by the FA and sent back to the home agent which then decapsulates them and forwards them as normal IP packets. Mobile-IP requires that each time a mobile device moves between points of attachment crossing a network or subnet boundary, it receives a new care-of address, and re-registers with its home agent. Home agents associate a lifetime to the state they install for a mobile, requiring periodic *lifetime renewals* to avoid state expiration and removal.

3.2. DHCP Overview

DHCP has a client-server architecture. The DHCP server manages a portion of the IP address space on a network by dynamically disbursing IP addresses and other associated configuration parameters to DHCP clients, such as name server IP addresses, on a request basis. A DHCP client running on a host allows it to dynamically acquire IP configuration state, replacing conventional static configuration methods where parameters are manually hard-coded into a host. If there are no DHCP servers on the same subnet to which the host is connected, a DHCP relay is introduced for forwarding client requests to servers on other subnets.

A key aspect of DHCP is that configuration parameters acquired by a client are leased, i.e., they have an associated expiration time so they must be periodically renewed in order to keep the lease from expiring. A DHCP client state machine generates lease renewals, sends them to the server and waits for acknowledgements before it renews its local leased configuration state. Unacknowledged lease renewal requests eventually cause lease expirations at the client with the subsequent mandatory removal of its configuration state.

DHCP client transactions take place in two stages. In the lease a*cquisition* stage, a mobile host has no home address configuration and it is strictly concerned with completing a full initialization. In the lease *maintenance stage,* the mobile host has a non-expired home address lease and it is concerned with keeping the lease from expiring. The DHCP standard specifies four salient client states regarding its association to an address lease, namely, INIT/REBOOT, BOUND, RENEWING and REBINDING. The first two states are associated with the lease acquisition stage while the latter two are concerned with lease maintenance. When a DHCP client state machine is initialized, it attempts to acquire a lease in the INIT/REBOOT state and then moves to the BOUND state on success. Internal client timers trigger the periodic lease renewals by trying to unicast to the serving DHCP server in the RENEWING state or using broadcasting as a fallback in the REBINDING state.

4. Mobility and DHCP: The Broadcasting Problem

Consider a model where mobile hosts rely on DHCP to dynamically configure both their home address and their co-located COA. This implies that DHCP clients running on the MH acquire and maintain leases on these two addresses. Let us refer to the DHCP client for the home address as Hclient and the DHCP client for the COA as Fclient.

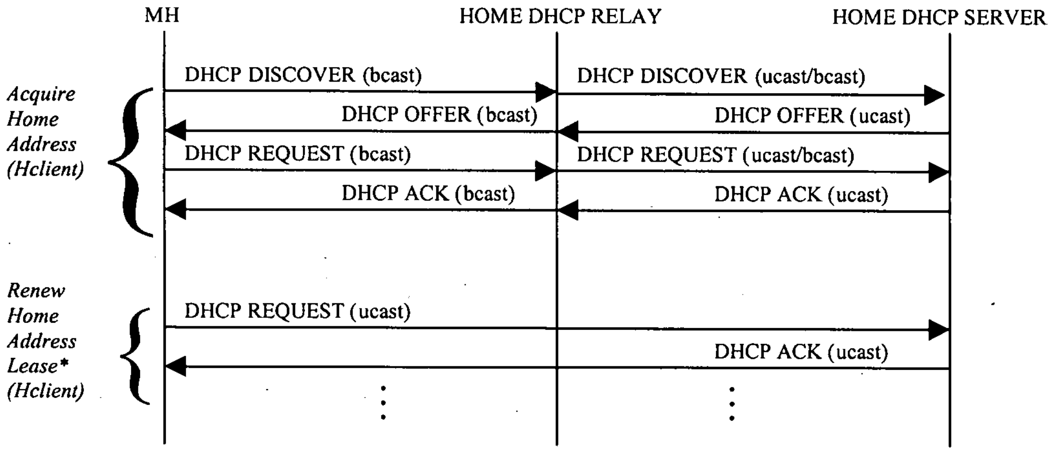

Figure 1. Procedures for Mobile Host Power-Up at its Home Network

Assume a mobile host powers up in its home network with no knowledge of an unexpired home address lease. Since it needs to acquire a home address, it initiates the execution of Hclient which must go through a full initialization (i.e., not a quick reboot). As shown in Figure 3, Hclient attempts to contact a DHCP server by broadcasting a DHCPDISCOVER message on its local subnet. This is actually a limited broadcast message since it is destined to IP address 255.255.255.255. The message is received by a DHCP server or a DHCP relay on that subnet that is configured to forward the message to a DHCP server elsewhere on the home network (the scenario shown involves a DHCP relay). When the message reaches the DHCP server, it responds with a DHCPOFFER that it either broadcasts on its subnet or unicasts to the relay that had forwarded it. Whether through the relay or directly from the server, the MH receives the message as a limited broadcast. Hclient then broadcasts a DHCPREQUEST, reaching the server directly or via the relay, as before. The server responds with a DHCPACK confirming the granting of a DHCP lease. The DHCPACK reaches the MH once again as a limited broadcast and Hclient concludes its lease acquisition stage by installing acquired state on the MH's IP interface. Hclient periodically enters the lease maintenance stage where it sends renewals to its home DHCP server. (The asterisk * in the figure means that the transaction is periodically repeated). As per the standard, no M-IP registrations are needed while the MH is in its home network.

Now let us consider the case where the MH powers up in a foreign network. Once again, assume, without loss of generality, that the MH holds no unexpired home address leases. If Hclient attempts to send a limited broadcast message in the hope of contacting a DHCP server that can grant it a home address, it will fail. Any upstream DHCP broadcast messages will be received by a local DHCP server or relay which will offer an address from its own lease pool, not that of the MH's home network. Home addresses can only be granted by DHCP servers in the MH's home network. Hclient needs a way to contact its remote home DHCP server, as standard DHCP broadcasting procedures will not enable a proper server discovery.

Contrary to the operation of Hclient, the standard broadcasting procedures of DHCP properly enable Fclient to acquire and maintain address leases for the MH's COA. This is because it is never the case that DHCP messages generated by a Fclient have to cross administrative network boundaries to reach the proper DHCP server for lease acquisitions or renewals.

In brief, standard DHCP broadcasting procedures do not work for dynamic home addressing on mobile hosts that power up in a foreign domain. DHCP messages sent by a MH client cannot reach a remote home DHCP server to acquire or renew a home address lease.

5. DHCP+M-IP: The Solution

While there are many possible ways to bridge the gap between a MH powering up in a foreign network and its remote home DHCP server, the notion of an addressing agent for home address allocation coupled with the assistance of M-IP is attractive and conducive to a viable solution. In this section, we describe our solution, referred to as the *Transient Tuneling Procedure* (TTP). The general idea is to use: a) M-IP as the signaling mechanism for reaching the home network and triggering the acquisition of a home address; b) an addressing agent in the home network to allocate a temporary home address for the MH; and c) DHCP to allocate valid home configuration state for the MH. Variations in the design of the addressing agent and its interaction with M-IP and DHCP leads to several possible solutions. We argue that TTP has superior benefits because it requires minor changes to protocol standards and deployed servers and it leverages the growing base of DHCP technology with its embedded support for DHCP configuration options beyond IP addressing. A discussion of alternative solutions is presented in Section 7.

Our approach is as follows. On power-up, we assume a MH is capable of determining whether it is in its home or in a foreign network. This location inference may be based on knowledge of its NAI, such as a user email address, or on the use of a wireless link-layer identifier (e.g., a Mobile Identification Number or MIN). Note that support for resolving a wireless link-layer identifier to a NAI may also exist [10]. Methods for location inference are not described in this paper and are an open research issue. As an example, however, a M-IP client on the MH may listen for periodic advertisements from a HA or FA containing the domain name which it can then compare against its own NAI.

Detailed message flows illustrating the ensuing power-up and mobility procedures are presented in the following two sections. Recall that although we assume the FA is co-located on the MH, the issue of co-location does not affect TTP. Minor changes concerning the use of an external FA are discussed in Section 8.

5.1. Power-Up Procedures

Recall that procedures for powering up in a home network were described in Section 4. Now consider the case when a MH determines it is powering up in a foreign network. As shown in Figure 4, the MH first needs to acquire a co-located COA so it spawns a DHCP client (Fclient). Once it acquires the COA, it sends a unicast M-IP registration message to its HA, assumed to be known through static configuration or some other means such as dynamic home agent address resolution[1][5]. The registration message contains the MH's COA and its NAI, but no home address. When the HA receives the registration message and notices that the home address is missing, it contacts a local addressing agent to acquire a home address for the MH.

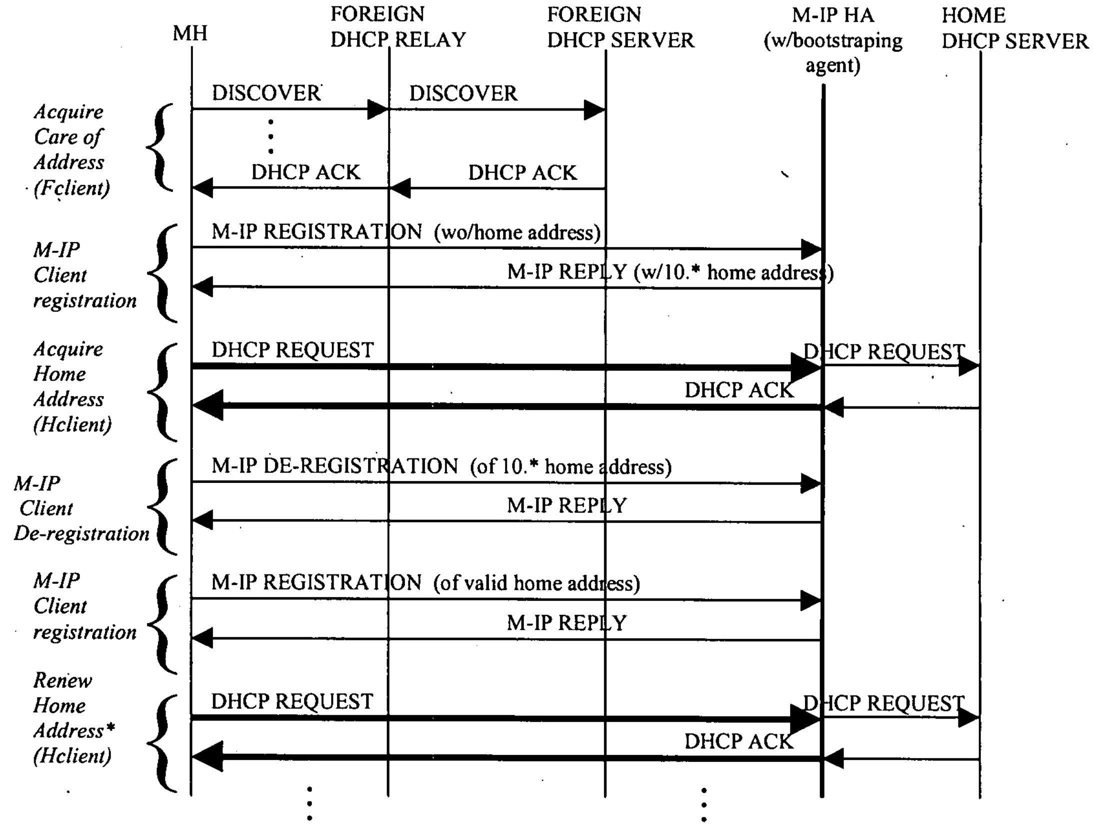
MH
FOREIGN DHCP RELAY
FOREIGN DHCP SERVER
M-IP HA (w/bootstraping agent)
HOME DHCP SERVER
Acquire Care of Address (Fclient)
DISCOVER
DISCOVER
DHCP ACK
DHCP ACK
M-IP Client registration
M-IP REGISTRATION (wo/home address)
M-IP REPLY (w/10.* home address)
Acquire Home Address (Hclient)
DHCP REQUEST
DHCP REQUEST
DHCP ACK
M-IP Client De-registration
M-IP DE-REGISTRATION (of 10.* home address)
M-IP REPLY
M-IP Client registration
M-IP REGISTRATION (of valid home address)
M-IP REPLY
Renew Home Address* (Hclient)
DHCP REQUEST
DHCP REQUEST
DHCP ACK

Figure 2. TTP for a Mobile Host Power-Up in a Foreign Network

We investigated several designs for the addressing agent, differing in implementation complexity.

[1] Dynamic home agent address resolution requires the MH to know the broadcast address for its home subnet.

Due to its implementation simplicity, we chose the design of a lightweight addressing agent referred to as a *bootstraping agent* and placed it on the M-IP HA. This bootstraping agent disburses temporary home addresses from a pool of private IP addresses of the class 10.*. Once a 10.* address is assigned, the M-IP HA uses it to set up a tunnel to the COA of the MH. The HA unicasts a registration reply message containing the 10.* address back to the MH. On receipt, the MH sets up its end of the IP tunnel. With the tunnel in place, a DHCP client (Hclient) is initialized on the MH and launches a standard set of transactions needed to acquire a IP home address and other DHCP options. All DHCP client messages must be reverse tunneled to ensure that they are not received by any local DHCP servers nor relays. Reverse tunneled messages are forwarded on the home subnet by the M-IP HA, so that a home DHCP server or relay receives them. Similarly, DHCP replies sent by a home server or relay are tunneled to the remote MH. Using the M-IP tunnel, Hclient successfully acquires an address (and possibly other configuration state) from a home DHCP server without concerns about broadcasting. After this bootstraping phase, the 10.* address should be released, its associated M-IP tunnel is torn down and replaced with a tunnel terminating at the DHCP-acquired home address[2]. This process entails a M-IP de-registration message from the MH to the HA, followed by a M-IP registration containing the valid home address. This solution also addresses the broadcasting problem associated with lease renewals, because they are likewise reverse-tunneled to the home network.

To ensure that DHCP replies from the server or relay in the home network reach the Hclient on the MH while it is in the foreign network, the client must set the broadcast bit "B" in the flags field of its DHCP query messages. Note that existing implementations of DHCP clients such as on Microsoft Windows and ISC's implementation for FreeBSD, always set the broadcast bit by default. By setting the broadcast bit, the client informs the DHCP server and relay that it cannot respond to unicast link-layer messages so it requires link-layer broadcasts. A server or relay should examine the broadcast bit and if set, should send any DHCP replies to the MH as an IP broadcast using an IP broadcast address as the IP destination address and the link-layer broadcast address as the link-layer destination address. This ensures that the HA receives broadcast packets for subsequent forwarding to the MH. To ensure that the HA tunnels these IP broadcasts to the MH, the M-IP client on the MH must also set the broadcast "B" bit in its M-IP registration request. In addition, the M-IP client must also set the "D" bit in its registration request to inform the HA that the MH is using the colocated COA option so the HA tunnels the broadcast messages directly to the MH's COA.

A drawback in setting the broadcast bit is that the MH may receive a flood of unwanted broadcast messages from its home network that are forwarded by the HA. This would result in a significant waste of wireless bandwidth. Strategies to address this issue are discussed in Section 8.

To summarize, TTP uses a bootstraping addressing agent on the HA to allocate private home addresses. This enables a temporary M-IP tunnel to be established to the MH over which a standard DHCP client on the MH can acquire a lease from a pool of public (i.e., globally routable) IP home addresses. Once a home address is acquired, it is used to replace the temporary tunnel with a corresponding M-IP tunnel.

5.2. Mobility Procedures

We now provide a detailed description of the operation of DHCP and M-IP required for a mobile host to establish and maintain connectivity as it moves. The message flows described conform to the standard operation of DHCP and M-IP.

[2] Alternative and more efficient methods for avoiding the explicit de-registration of the 10.* binding require more study.

Moving into a foreign network: First, the MH must acquire a co-located COA. As illustrated in Figure 5, the MH initiates a DHCP client process, Fclient, to acquire and maintain a COA from a DHCP server in the foreign domain according to standard procedures. Once the COA is acquired, the M-IP client on the MH sends a registration message to its HA to establish a tunnel from the MH's home address to its COA. This registration message contains the mobile's home address. When the MH receives a reply message from its HA, its co-located FA sets up its end of the tunnel thus completing reestablishment of the data path to the MH.

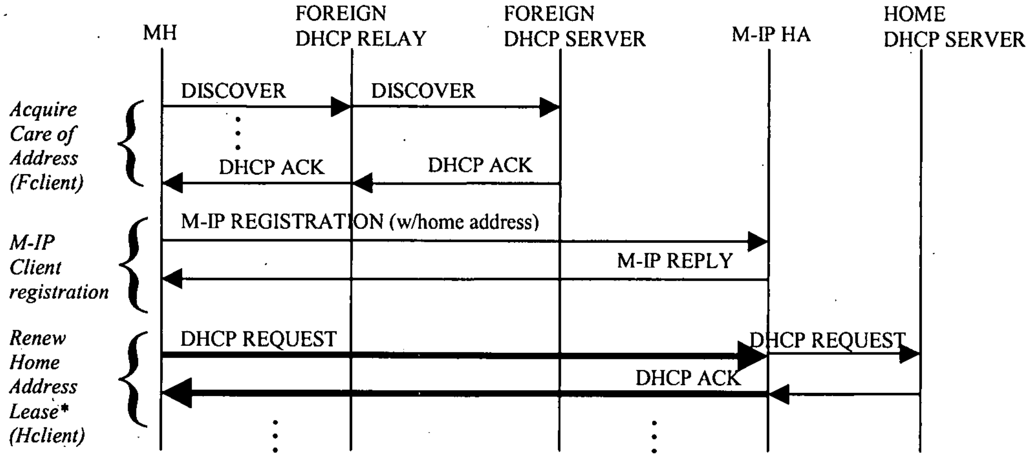

Figure 3: Procedures for a Mobile Host Moving out of its Home Network

Upon entering the foreign network, the Hclient process running on the MH must continue to renew the home address lease by sending DHCP messages via the M-IP tunnel. The HA will decapsulate these packets and forward them in the home network. This approach is firewall-resistant so it enables unicast delivery as well as broadcast delivery (whether limited or subnet-directed). Although not shown in the figure, Fclient must also send periodical renewal messages to prevent the COA from expiring.

Some inter-process synchronization may be needed to ensure that M-IP has completed setting up the tunnel before Hclient attempts to send a lease renewal. A precautionary measure to prevent the unlikely event of a home address lease expiration during a handoff is to force Hclient to send a lease renewal just prior to leaving its home network. This works because the interval between lease renewals is much greater than the time it takes to complete a handoff, but it requires advance notification of an impending handoff, which may not be viable depending on the underlying link layer technology.

Note that the two DHCP clients, Hclient and Fclient, and the M-IP client must all operate succesfully for the MH to establish and maintain its connectivity in the foreign network. The failure of any of these processes leads to a configuration failure for the host. Should this occur, the mobile host may attempt a reboot and reinitialization as if it were in its home network. Issues regarding the design of policies for handling configuration failures are a subject for further study.

Moving into the home network: Procedures for this scenario are illustrated in Figure 6. When the MH enters its home network, its M-IP client should send a de-registration message to its HA in order to tear down the existing tunnel to its former COA. No further M-IP transactions are conducted while the MH remains in its home domain. The DHCP Fclient on the MH should release the COA by unicasting a DHCPRELEASE message to the DHCP server in the foreign network. If the message is sent from the home network, the presence of a firewall may prevent it from reaching the proper foreign DHCP server. Failure to send a DHCPRELEASE will eventually result in the server's release of the COA on lease expiration. After the release is sent, Fclient must no longer conduct any DHCP transactions and the process is halted. Hclient continues to send periodic lease renewals, no longer requiring the services of a M-IP tunnel to reach home DHCP servers.

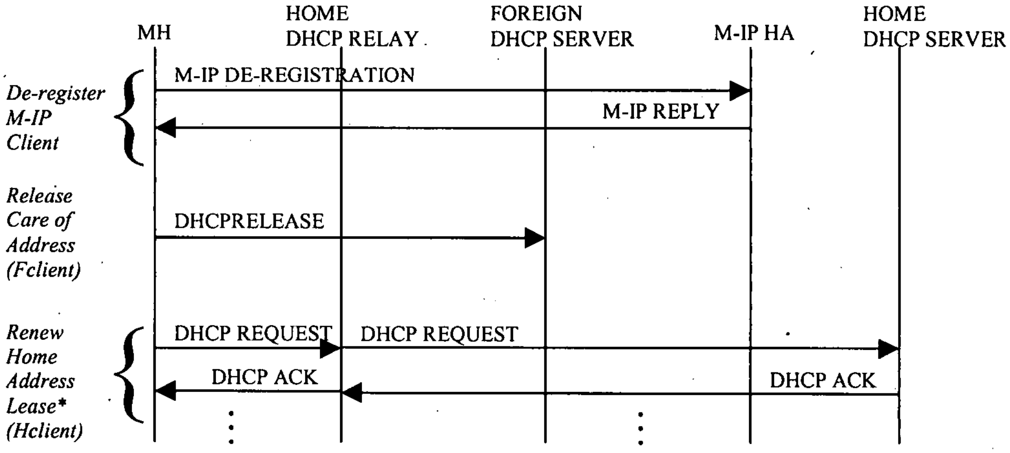

Figure 4. Procedures for a Mobile Host Returning to its Home Network

6. Implementation and Performance

We implemented our solution on a wireless access network testbed comprising Pentium-based PCs running FreeBSD. The mobile host was a Pentium laptop running Linux, and equipped with a 6 Mbps WaveLAN PCMCIA card. Our network configuration is shown in Figure 7. Access routers in the home and foreign networks were configured as WaveLAN base stations and DHCP relays. We used the FreeBSD ISC implementation of DHCP (version 2) [8] for the server, client and relay. For Mobile-IP, we used our own implementation of a home agent on a Lucent IP router. We also used our own implementation of a M-IP client supporting foreign agent co-location. Our M-IP implementation was properly verified to comply with the standard.

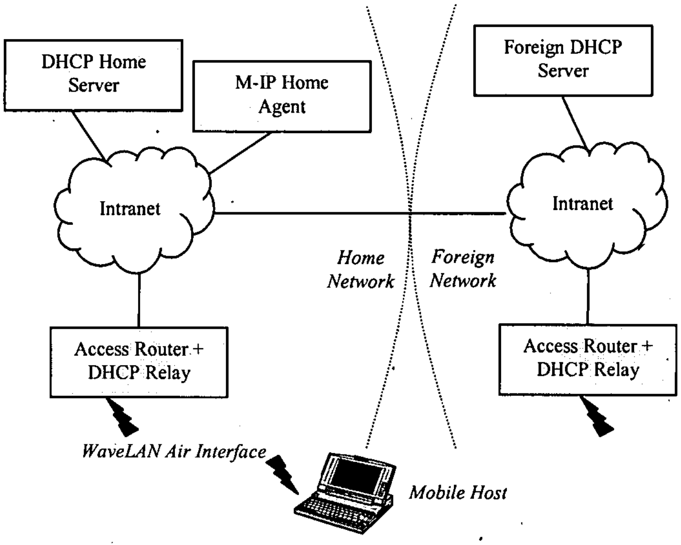

Figure 7. Implementation Testbed Network

We verified the correctness of the procedures for mobile host power-up and mobility previously discussed. These scenarios included powering up at home or in a foreign network and crossing a network boundary. As anticipated, modifications needed to the standard DHCP and M-IP codebase to support our solution did not require significant implementation effort and provided some insights worth noting. Observations regarding Home Agent operation follow:

- *Multi-homing:* A clarification in the M-IP specification is needed regarding the forwarding treatment of incoming tunnelled broadcast packets at the Home Agent. When a HA has multiple interfaces (e.g., for multi-homing), there must be an association between the M-IP client's NAI and the HA's interface on the client's home network. This is needed by the HA to identify on which interface to forward the broadcast packets after de-capsulation.

- *Client Address Filtering:* Security measures typically prevent the HA from forwarding tunneled broadcast packets when the sending M-IP client has a home address that is inconsistent with the network where the HA resides. This security feature needs to be disabled to support clients with 10.* addresses.

- *NAI-based indexing:* The HA maintains a security-association list to describe the bindings of mobile hosts to their shared key for authentication. While mobile hosts may be identified by a home address or, as of recent, a NAI, this list is indexed by home addresses. In cases where authentication must proceed without knowledge of a client home address, indexing must be done using the NAI.

[Summarize the changes/modifications to M-IP and DHCP required to enable our solution: DHCP(none), M-IP(bootstraping agent, disabling of client address filtering, nai-based indexing, multi-homing support, extension of MIP registration message to include MAC address and of M-IP reply to include home address, optional selective enabling of the HA tunneling of broadcast packets)]

[Performance evaluation: Two types of measurements to report –

- Power-Up latencies – Measure TTP latency = COA setup + MIP_REG (10.*) + HomeAddr setup + MIP_DEREG + MIP_REG (HomeAddr). Assess the overhead for transient tunnel setup and justify it based on a power-up scenario. Measure and compare with the latency of a power-up at home.

- Inter-domain handoff latencies – Measure and compare latency of home -> foreign, foreign -> home and foreign -> foreign handoffs with respect to DHCP and M-IP setup. Contrast with power-up latencies (the handoff latencies will hopefully be much smaller). Discuss means to reduce handoff latency (similar to the Maguire study). If time permits, it would be nice to include a discussion about how these latencies affect the application layer.]

7. Alternative solutions

As stated earlier, there are several possible ways to design the addressing agent. Contrasting with our proposed bootstraping agent, we also examined the notion of an *embedded agent* and a *proxy agent,* described as follows.

In the *embedded agent* approach, the allocation of home addresses for hosts powering up away from home is completely up to an addressing agent embedded within a M-IP Home Agent. In other words, DHCP is excluded from the addressing process. The sophistication of this embedded agent may range from providing lighweight addressing support similar to our bootstraping agent to a rich-featured DHCP-like server engine. In the case of a lightweight addressing agent, it differs from the bootstraping model because it manages a pool of addresses reserved from within the public IP address space of the home network. The same applies to a rich-featured embedded agent, which may additonally provide soft-state support and the allocation of other configuration parameters besides addresses (analogous to DHCP options).

In the *proxy agent* approach, the addressing agent acts like a surrogate DHCP client for the MH. It conducts a standard DHCP transaction in the home network to acquire a home address for the mobile (with no options) from a local DHCP server. It does so by behaving like a co-located DHCP client and relay; it behaves like a client masquerading (through MAC address spoofing) as the MH and like a relay to DHCP servers residing on the home network. This requires that the MH includes its MAC address in the M-IP registration message sent after power-up. The MAC address is needed because it is the MH identifier used by a DHCP server to associate with its lease records. On receipt of the registration message, the HA contacts the proxy agent and conveys to it the MH's MAC address. The proxy agent spawns a DHCP client state machine modified to send and receive DHCP messages to and from a local DHCP server as if it were passing through a relay. After the proxy acquires a home address, it halts the client state machine (i.e., aborts lease maintenance procedures) and conveys the addressing information to the HA. The HA, in turn, creates a tunneling entry for the mobile using its known COA and acquired home address, then forwards the home address to the MH in its registration reply message. When the MH receives the reply, it installs the home address on its interface, and sets up its tunnel endpoint (managed by its co-located Foreign Agent). Once the tunnel is in place, the MH spawns a DHCP client and immediately renews its home address lease, requesting any other DHCP options of interest. In this manner, the proxy agent only manages home address acquisition while the DHCP client on the host carries out lease maintenance transactions. Note that if the home DHCP server address is also piggybacked on the registration reply from the M-IP HA, the DHCP client on the MH may attempt to renew its lease via unicast DHCP request messages destined to the home server.

The disadvantage of embedded agents is that they potentially require substantial modifications to M-IP Home Agents to duplicate part or most of the functionality already provided by DHCP. In addition, they require a partitioning of the home network address space between DHCP servers and M-IP Home Agents, representing an administrative burden and possibly introducing space fragmentation inefficiencies. Unlike embedded agents, proxy agents rely on the use of DHCP for home addressing. Proxy agents provide a loose coupling between M-IP and DHCP by strictly limiting the addressing role of a HA to be that of a mediator between the MH and the proxy. Their shortcomings lie in the complexity of implementing the proxy, building an interface between the proxy and the HA, modifying the HA to perform its mediating role, and commiting to future HA updates to reflect changes in the evolution of DHCP . Another issue is that future security enhancements to DHCP may preclude the use of MAC address spoofing. Although the effort to implement proxy agents is not unreasonable, it is substantially greater than the task of building bootstraping agents.

8. Other Important Issues

A discussion of several issues related to our work follows. Specifically, we discuss issues concerning the *efficient use of wireless bandwidth,* the use of *external foreign agents* instead of MH co-location, and implementation considerations pertaining to the support *of multiple DHCP clients on a single host interface.*

Efficient Wireless Bandwidth Usage: Mobile hosts usually connect to an IP access network through a wireless air link, where bandwidth tends to be limited and costly due to physical and regulatory constraints. As a result, practical mobility solutions should be concerned with the effective use of air bandwidth. Typical approaches to address this concern are packet header and payload compression techniques and the reduction of over-the-air traffic.

In addition to packet payload compression methods [22], there has been a considerable amount of work on the compression of a variety of packet headers including IP, TCP, UDP, IP-in-IP, RTP and PPP [23, 20, 21]. Though the compression of UDP-based DHCP and M-IP control packets has not explicitly received attention, similar compression techniques might be applied. The investigation of compression ratios for these packets is an open issue.

Efforts to reduce traffic over-the-air take several forms, distinguished as *bandwidth waste prevention* and the *reduction of control message frequency.* One way to prevent bandwidth waste in TTP is to stop unwanted broadcast packets originating in the home network from being tunneled to the MH by its HA. Recall from Section 5.1 that a broadcasting option needs to be set in the HA so that DHCP packets broadcast by a server or relay in the home network reach the MH in a foreign network. Unfortunately, all broadcast packets will be forwarded, not just the few desired DHCP packets. An approach to alleviate this problem is to perform a selective enabling of the tunneling of broadcast messages only during the relatively short intervals during which DHCP transactions are needed. While this significantly reduces bandwidth waste, it may still be unacceptable for very low bit-rate wireless links.

For example, consider the HA has 10,000 mobile suscribers with an average of 3 suscribers powering up each second. Assume that DHCP configuration latency is on the order of 5 seconds (a pessimistic estimate), and that broadcasting is enabled only during this interval. In this interval, 15 suscribers will power up, each of them expecting to receive at least 2 DHCP broadcast packets (an OFFER and an ACK) from a home DHCP server. With a typical DHCP packet size of 512 bytes, this represents a total traffic overhead of 15 KB (or 24 Kbps) being sent over the wireless link of *every* MH while they attempt to power up away from home. With current wireless WAN bit-rates on the order of 9.6 Kbps, this overhead is out of the question. Tomorrow's wireless WAN bit-rates on the order of 100 Kbps and greater will mitigate but not eliminate the problem.

A performance optimization for TTP that eliminates this problem is to disable the tunneling of broadcast packets from the HA altogether and to force the DHCP home server to reply to the MH with IP unicast messages. This can be done by modifying the DHCP client on the MH to appear as though it were sending its messages through a DHCP relay, as the standard specifies that relayed messages be unicast to the relay. This "virtual relay" on the DHCP client would use the private home address of the MH acquired through TTP as its IP address and advertise it to the server in DHCP requests (in the 'giaddr' field).[3] Unicast DHCP replies would likewise be processed through this virtual relay to eliminate relay state and hand it off to the DHCP client for normal processing. This approach hinges on the fact that TTP assigns a private home address that can be used to simulate relay functionality for acquiring the home address through DHCP. A shortcoming of this approach is that it requires a DHCP server to be on the same subnet as the M-IP HA, because a relayed DHCP request cannot go through more than one relay on its way to a server. Observe that replies to DHCP lease renewal requests are unicast to the MH so they do not need tunneling support for broadcast messages.

A similar bandwidth waste may be introduced during the power-up of MH's in their home network. Depending on how IP broadcasts are handled over specific wireless link technologies, they could be bandwidth-intensive. To avoid such problems in DHCP, we recommend that, when possible, a MH powering up in its home domain clears the broadcast bit in the flags field of its DHCP query messages. This is only possible for hosts that are able to receive unicast IP datagrams before their protocol software has been configured with an IP address. Clearing the broadcast bit informs the DHCP server and relay of the client's wishes to receive unicast messages rather than broadcasts. A server or relay should examine the broadcast bit and if clear, should send any DHCP replies to the MH as an IP unicast using the IP address specified in the 'yiaddr' field and the MH's link-layer address specified in the 'chaddr' field.

As stated earlier, the reduction of control message frequency is another way to reduce over-the-air traffic. To achieve this, administrative measures may be taken such as constraining periodic broadcasting (e.g., beaconing) intervals for foreign agent discovery on the downlink and supporting long DHCP lease renewal times and M-IP registration lifetimes for uplink traffic. Another strategy to reduce over-the-air control traffic is to migrate client functionality from the MH onto an element in the access network. This element performs most of the required signaling on behalf of the mobile, at the expense of added network complexity. Note that the use of a M-IP foreign agent does not follow this strategy because an FA plays a mostly passive role in M-IP registration while client functions are still controlled by the MH. However, the idea of client migration may be applied to dynamic home addressing. As an example, consider that the definition of a proxy agent given in Section 7 is extended to include support for DHCP lease maintenance. Assume a MH only has a M-IP client which it must always use M-IP to trigger the acquisition of a home address regardless of where it is powering up (conflicting with standard M-IP registration procedures). A home address may be acquired and installed by the M-IP client through a registration, while the proxy agent in the home network assumes indefinite responsibility for lease maintenance. A lightweight signaling protocol (yet to be defined) between the M-IP HA and the proxy agent would allow the HA to trigger address acquisition, enable the HA and a MH to be notified of a failed lease renewal and enable the proxy to be

[3] Address assignment rules used by the DHCP server to decide which address to assign to an incoming request are not standardized. Server implementations often select an address on the subnet where the relay resides, if the request was relayed, or on the subnet associated with the server's interface on which the request was received. This may yield an undesirable address assignment for TTP, entailing possible implementation-dependent changes to the server's subnet selection rules.

notified when the MH no longer requires its services (e.g., on power-down). This approach keeps lease renewals localized regardless of MH mobility but could turn the proxy agent into a bottleneck as it must run a client state machine for every active MH belonging to this home network. Moreover, as stated earlier, the proxy may not be able to use MAC address spoofing for security reasons. There are other ways to support client migration for dynamic home addressing not discussed in this paper. In general, the complexity of these solutions is unjustified for most wireless networking scenarios because the potential air bandwidth gains are marginal.

Multiple DHCP Clients per Host Interface: Current DHCP client implementations such as ISC's [8] allow a host with multiple network interfaces to dynamically configure each interface. Concurrently executing DHCP client state machines on the host acquire, install, and maintain configuration state for each interface without interfering with each other. However, the support of more than one DHCP client for a single interface requires that steps be taken to prevent or resolve any resource conflicts that may arise on the shared interface, such as during the installation of acquired configuration state. These potential conflicts raise implementation-dependent issues that must be addressed if mobile hosts are to dynamically configure their home and care-of address, typically on a single wireless interface.

External Foreign Agents: An underlying goal for our work was to enable mobile hosts to dynamically configure both their home address and their co-located care-of address. Regardless of whether or not co-location is used makes no difference to TTP, with the exception of an issue regarding FA support for private home addressing.

The use of private home addressing with M-IP, as required by TTP, raises potential MH address collisions at the foreign agent. Since by definition private addresses are not globally unique, it is possible than an overlap occurs between the private addresses of MH's belonging to different HA's but served by the same FA. To resolve such addressing conflicts and ensure proper routing to the MH's, the FA must use additional MH configuration state such as the NAI or the HA IP address. This address conflict resolution is an open issue currently being addressed [18,19].

Other noteworthy observations to be made regarding the general use of external foreign agents relate to their effect on *care-of address setup delay* and on *packet size over wireless links*. On the former issue, the delay for acquiring a COA from an FA may be significant. Though such a delay should in principle, be negligible, current implementations of the Agent Solicitation and Agent Advertisement handshake required between the MH and the FA to acquire the COA are slow because they run in user space. The configuration delay when using an FA has been shown to be larger than if the co-located FA option with DHCP addressing is used [2]. This configuration delay has a negative impact on handoff latencies.

A benefit of using external FA's is that it reduces the size of all packets over the wireless link. This is because the FA terminates the M-IP tunnel originating at the HA by decapsulating and encapsulating all packets to and from the MH. Packet header sizes over the wireless link are reduced as the outer IP layer added for encapsulation is only used in the access network. The wireless bandwidth gains are nonetheless of questionable value because IP-in-IP header compression techniques using minimal encapsulation have reduced the header overhead for co-location to 2 bytes. This overhead is negligible with respect to packet sizes ranging from 200 to 300 bytes on the average up to a maximum size (MTU) of 1500 bytes.

Ipv6 Considerations:

Configuration latency: (to be written after the performance discussion is done)

9. Summary and Future Work

In this paper, we closely examined the problem of dynamic configuration for mobile hosts and focused on solving an important problem in enabling DHCP to be used as the protocol for host addressing and configuration. DHCP's reliance on broadcasting to enable server discovery by mobile hosts does not work when these hosts power up in a foreign network and try to acquire a home address through DHCP. We introduced the *Transient Tuneling Procedure* (TTP) as a solution to this problem, comprising a two-stage addressing procedure. In the first stage, a transient M-IP tunnel is established to the MH using a private home address and standard DHCP transactions are conducted over the tunnel to acquire a globally routable home address. In the second stage, the transient tunnel is replaced with a new one using the DHCP-acquired home address. TTP is built on the notion of a *bootstraping agent* in the home network capable of allocating private home addresses. This addressing agent is indirectly reachable by the MH through its M-IP Home Agent. We defined the set of message flows used by TTP as well as the standard DHCP and M-IP procedures for a mobile host to power up in its home network and move across network boundaries. We discussed other related issues impacting dynamic addressing such as wireless bandwidth usage and the use of external Foreign Agents.

Our implementation of TTP on a networking testbed showed...TBA.

Although we described alternative dynamic configuration solutions that do not rely on DHCP, we argue that TTP has superior benefits in its ability to leverage the growing base of DHCP technology and its embedded support for important and often necessary configuration options beyond IP addressing (e.g., subnet mask). TTP requires minor changes to protocol standards and deployed servers, amounting to a few enhancements to the M-IP protocol and Home Agents. While being DHCP-based, TTP is potentially useful to any dynamic addressing protocol that, like DHCP, relies on broadcasting for server discovery.

An interesting subject for further study is the definition of APIs for the inter-process communication of co-located M-IP and DHCP agents. Potential benefits of co-locating DHCP servers and M-IP Home Agents include the ability to reduce M-IP registration latency [1], to indirectly trigger DHCP addressing transactions and to share security information. The co-location of DHCP and M-IP clients on mobile hosts could also benefit from the existence of an API that would, for instance, allow M-IP to alert DHCP of an impending handoff. That way DHCP can release a co-located COA it no longer needs rather than having to rely on its lease expiration. By the same token, DHCP could inform M-IP of a forthcoming transaction so that M-IP can re-enable the tunneling of broadcast packets from the home network. Similar benefits for co-locating Foreign Agents and DHCP relays should be examined. In brief, the creation of these API's may result in performance improvements and dissuade protocol designers from introducing functional redundancies across these protocols (e.g., placing handoff detection support into DHCP).

References

1. Using DHCP with Computers that Move, Charles Perkins and Kevin Luo, Wireless Networks Journal, vol. 1, pp. 341-353, 1995
2. The effect of using co-located care-of addresses on macro handover latency, Jon-Olov Vatn and Gerald Maguire Jr., in Proceedings of Nordic Teletraffic Seminar, August 1998

3. Long random wait-times for getting a care-of address are a danger to Mobile Multimedia, Jon-Olov Vatn, IEEE Intl. Workshop on Mobile Multimedia Communications, pp. 142-144, Nov. 1999
4. Mobile IP Network Access Identifier Extension for IPv4, Pat Calhoun and Charles Perkins, draft-ietf-mobileip-mn-nai-07.txt at www.ietf.org, January 2000
5. IP Mobility Support, Charles Perkins, RFC 2002, October 1996
6. Dynamic Host Configuration Protocol, R. Droms, RFC2131, March 1997
7. Route Optimization in Mobile IP, Charles Perkins and David Johnson, http://search.ietf.org/internet-drafts/draft-ietf-mobileip-optim-08.txt, February 1999
8. Internet Software Consortium (ISC), http://www.isc.org
9. DHCP Options and BOOTP vendor Extensions, S. Alexander and R. Droms, RFC2132, March 1997
10. NAI Resolution for Wireless Networks, Aravamudhan, O'Brien and Patil, URL:draft-aravamudhan-mobileip-nai-wn-00.txt, October 1999
11. The Subnet Selection Option for DHCP, G. Waters, June 99, http://www.ietf.org/internet-drafts/draft-ietf-dhc-subnet-option-03.txt
12. Dynamic Registration and Configuration Protocol (DRCP), A. McAuley, S. Das, S. Baba and Y. Shobatake, http://search.ietf.org/internet-drafts/draft-itsumo-drcp-00.txt, October 1999
13. Interaction between DHCP and DNS, M. Stapp and Y. Rekhter, http://search.ietf.org/internet-drafts/draft-ietf-dhc-dhcp-dns-11.txt, October 1999
14. DHCP Configuration of IPSEC Tunnel Mode, B. Patel, B. Aboba, S. Kelly and V. Gupta, http://search.ietf.org/internet-drafts/draft-ietf-ipsec-dhcp-04.txt , Expires: Aug. 2000
15. Extensions for the Dynamic Host Configuration Protocol for IPv6, C. Perkins and J. Bound, http://search.ietf.org/internet-drafts/draft-ietf-dhc-v6exts-11.txt, Feb. 1999
16. Authentication for DHCP Messages, R. Droms and W. Arbaugh, http://search.ietf.org/internet-drafts/draft-ietf-dhc-authentication-12.txt, October 1999
17. Mobility Support in IPv6, David B. Johnson and Charles Perkins, draft-ietf-mobileip-ipv6-07.txt, November 1998.
18. Private Addresses in Mobile IP, C. Perkins, G. Montenegro and P. Calhoun, http://search.ietf.org/internet-drafts/draft-ietf-mobileip-privaddr-00.txt, June 1999
19. Mobile IP extension for Private Internets Support (MPN), W. Teo and Y. Li, http://search.ietf.org/internet-drafts/draft-teoyli-mobileip-mvpn-02.txt, Feb. 1999
20. M. Degermark, B. Nordgren and S. Pink, "IP Header Compression," Internet Engineering Task Force RFC 2507, Dec. 1998.
21. S. Casner, C. Bormann and M. Engan, "IP Header Compression over PPP," Internet Engineering Task Force, RFC 2509, Dec. 1997.
22. M. Thomas, R. Monsour, R. Pereira and A. Shacham, "IP Payload Compression Protocol (IPComp)," Internet Engineering Task Force, May 1998.
23. Compressing TCP/IP Headers for Low-Speed Serial Links, Van Jacobson, RFC 1144, Feb. 1990
24. IP Encapsulation within IP, Charles Perkins, RFC 2003, Oct. 1996